the vehicle key if a vehicle is used to block the path.

(ii) Park the aircraft in a locked hangar and control the key to the hangar.

(iii) Move stairs away from the aircraft and shut and, if feasible, lock all cabin and/or cargo doors, and control the key.

(iv) Other means approved in writing by TSA.

(3) Verify background information of those individuals who are designated as the TSA point(s) of contact and those who have access to any keys or other means used to prevent the operation of large aircraft described in paragraph (b)(2) of this section by one or more of the following means:

(i) Verify an employee's employment history. The repair station obtains the employee's employment history for the most recent five year period or the time period since the employee's 18th birthday, whichever period is shorter. The repair station verifies the employee's employment history for the most recent 5-year period via telephone, email, or in writing. If the information is verified telephonically, the repair station must record the date of the communication and with whom the information was verified. If there is a gap in employment of six months or longer, without a satisfactory explanation of the gap, employment history is not verified. The repair station must retain employment history verification records for at least 180 days after the individual's employment ends. The repair station must maintain these records electronically or in hardcopy, and provide them to TSA upon request.

(ii) Confirm an employee holds an airman certificate issued by the Federal Aviation Administration.

(iii) Confirm an employee of a repair station located within the United States has obtained a security threat assessment or comparable security threat assessment pursuant to part 1540, subpart C of this chapter, such as by holding a SIDA identification media issued by an airport operator that holds a complete program under 49 CFR part 1542.

(iv) Confirm an employee of a repair station located outside the United States has successfully completed a security threat assessment commensurate to a security threat assessment described in part 1540, subpart C of this chapter.

(v) Other means approved in writing by TSA.

§ 1554.103 Security Directives.

(a) *General.* When TSA determines that additional security measures are necessary to respond to a threat assessment or to a specific threat against civil aviation, TSA issues a Security Directive setting forth mandatory measures.

(b) *Compliance.* Each repair station must comply with each Security Directive TSA issues to the repair station within the time prescribed. Each repair station that receives a Security Directive must—

(1) Acknowledge receipt of the Security Directive as directed by TSA;

(2) Specify the method by which security measures have been or will be implemented to meet the effective date; and

(3) Notify TSA to obtain approval of alternative measures if the repair station is unable to implement the measures in the Security Directive.

(c) *Availability.* Each repair station that receives a Security Directive and each person who receives information from a Security Directive must—

(1) Restrict the availability of the Security Directive and the information contained in the document to persons who have an operational need to know; and

(2) Refuse to release the Security Directive or the information contained in the document to persons other than those who have an operational need to know without the prior written consent of TSA.

(d) *Comments.* Each repair station that receives a Security Directive may comment on the Security Directive by submitting data, views, or arguments in writing to TSA. TSA may amend the Security Directive based on comments received. Submission of a comment does not delay the effective date of the Security Directive.